Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 11 December 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports five former Amtrak conductors working out of the Rensselaer station were sentenced for stealing money from the company, and ordered to repay the more than $120,000 they stole. (See item 8)
- Reuters reports the Food and Drug Administration officials have determined that a deadly outbreak of hepatitis A among restaurant diners in Tennessee, Georgia, and Pennsylvania was caused by green onions produced in Mexico. (See item 15)
- eWEEK reports security experts have found a new way to exploit a critical vulnerability in Windows that evades a workaround. (See item 21)
- Internet Security Systems has raised AlertCon to Level 2, due to a significant increase in UDP port 1433 (microsoft−SQL−Server) over the past 36 hours. (Please refer to the Internet Alert Dashboard)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *December 10, Associated Press* — **China and U.S. lead in demand for oil.** With China's economy expanding rapidly and a recovery simmering in other countries, demand for oil will

increase faster than expected this year and in 2004, the International Energy Agency (IEA) said Wednesday, December 10. **Demand has surged this autumn in the United States and several other industrialized nations, while Chinese demand appears to be advancing "at a breakneck pace," the agency said in its monthly oil market report. The global appetite for crude in 2003 will grow by a robust 1.9 percent,** or 1.44 million barrels a day, and in 2004 by 1.5 percent, or 1.16 million barrels a day. The IEA raised its estimates for daily demand growth in the two years by 160,000 barrels and 90,000 barrels, respectively. Paul Horsnell, head of energy research at Barclays Capital in London, agreed that China's thirst for oil imports has become a significant factor in global markets. China is a top oil importer after the United States, and both countries are leading the global economic recovery. **Oil prices remain high but volatile due to low inventories and geopolitical uncertainties ahead of the winter heating oil season.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A53271−2003Dec 10.html

[Return to top]

Chemical Sector

2. *December 10, WTOC TV (Savannah, GA)* — **Chemical leak closes streets. A chemical leak at a company in west Savannah had firefighters, police and other emergency officials scrambling overnight. Shortly after 2 a.m. Wednesday morning, residents in the area of East Lathrop and Bay Street reported some kind of chemical stinging their eyes. Hazmat authorities and other Savannah firefighters determined there was a leak at Natro−Chem,** a company on East Lathrop near Precinct One. Fire authorities say the leak was from a 55−gallon drum with a chemical that vaporizes when it reaches 120 degrees. It caused the alcohol−based chemical to form a cloud over the area. Savannah−Chatham police blocked off Bay Street to all traffic, and firefighters called the men who operate the company. An EMS unit was also called out to treat men on a freight train that had come through. East Lathrop was closed, but all streets have now reopened and everything appears to be under control.
Source: http://www.wtoctv.com/Global/story.asp?S=1558503&nav=0qq6Jad 1

[Return to top]

Defense Industrial Base Sector

3. *December 10, General Accounting Office* — **GAO−04−206: Satellite Communications: Strategic Approach Needed for DoD's Procurement of Commercial Satellite Bandwidth (Report). In recent years, the Department of Defense (DoD) has come to rely more heavily on commercial satellite communications to plan and support operations and move toward a network−centric warfare environment.** DoD acquires commercial satellite bandwidth services to support a variety of critical missions such as surveillance performed by unmanned aerial vehicles. **GAO was asked to assess (1) whether DoD's process for acquiring these services is fair to vendors and providers, (2) whether the process meets users' needs, and (3) whether spending on these services is managed effectively and efficiently. GAO's recommendations to DoD focus on the need to develop and implement a strategic approach to acquire commercial satellite bandwidth services, along with correcting**

specific oversight and management weaknesses. To ensure the successful implementation of a strategic management framework, GAO recommends that DoD develop performance metrics to assess user satisfaction, strengthen core internal technical expertise and information systems, and assess whether the existing acquisition process requires changes to facilitate a strategic approach. DoD generally concurred with GAO's recommendations. Report: http://www.gao.gov/cgi−bin/getrpt?GAO−04−206
Source: http://www.gao.gov/highlights/d04206high.pdf

4. *December 09, Federal Computer Week* — **Military sees network benefits from IPv6. The next generation of Internet standards will help the Department of Defense (DOD) reach its goal of network centricity, a DOD official said on Tuesday, December 9. IP version 6 (IPv6) will ultimately expedite the department's move toward network centricity, said John Osterholz,** DOD's director of architecture and interoperability. After the September 11, 2001, terrorist attacks, "our ability to come back online and handle operational matters was impaired," he said. "We needed to be more networked than we were, and we realized an important truth: The way we handle data on the network defeated the purpose of having the network in the first place." Information keepers distributed data to people they thought needed it but didn't consider that far more people could use the raw data in their work, specifically in warfighting, Osterholz said. **The fundamental limitations of IPv4, the protocol that has been in use for years, hinder network−centric operations, which link portions of the battlefield to provide situational awareness and knowledge superiority. IPv6 will let data travel more smoothly and efficiently.** John Stenbit, DOD's chief information officer, mandated that any hardware or applications acquired after October 30, 2003, must be IPv6 compatible.
Source: http://fcw.com/fcw/articles/2003/1208/web−ipv6−12−09−03.asp

[Return to top]

Banking and Finance Sector

5. *December 10, Government Computer News* — **Treasury kicks off new financial infrastructure protection effort. The Department of Treasury is investing $2 million to upgrade its Financial Services Information Sharing and Analysis Center to protect banks and the financial industry from cyberthreats. Treasury will also provide a liaison between the Department of Homeland Security and the financial sector beginning next week, Treasury Secretary John Snow said** Tuesday, December 9. The financial center has a secure database, analytical tools, and data gathering and distribution capabilities that let authorized individuals submit information−either anonymously or by name−about security threats. About 80 financial firms and organizations are members but they account for only 40 percent of the nation's assets and transactions, according to Treasury estimates. The goal of the upgrades is to give the center the ability to better serve the entire financial services sector. The center's database contains information about 4,300 threats, vulnerabilities and events dating back to 1999. **By 2005, the center wants to be capable of alerting 99 percent of financial organizations within an hour of a cyberthreat−such as a worm, virus or terrorist act−that might affect the financial industry.** The center would also recommend any necessary action.
Source: http://www.gcn.com/vol1_no1/daily−updates/24377−1.html

6.

December 10, finextra.com — **NatWest resumes normal service after phishing scare. The UK's NatWest bank has resumed normal service on the Internet after temporarily shutting down its online banking site following an attempted e−mail scam. The bank suspended service at its site on Monday, December 8, after some customers received spam e−mails** urging them to upgrade their account information at a bogus Web address. A bank spokesperson said that no customers appear to have lost any money as a result of the attempted fraud and that the site shut−down was a temporary precaution. NatWest was last hit by a similar 'phishing' expedition in October, during a rash of e−mail frauds targeting UK banks.
Source: http://www.finextra.com/fullstory.asp?id=10771

[Return to top]

Transportation Sector

7. *December 10, Department of Homeland Security* — **Department of Homeland Security announces $179 million in grants to secure America's ports.** The Port Security Grant Program provides resources for security planning and projects to improve dockside and perimeter security which is vital to securing our critical national seaports. These new awards will contribute to important security upgrades like new patrol boats in the harbor, surveillance equipment and the construction of new command and control facilities. **"The Department of Homeland Security is committed to further securing our nation's highways, mass transit systems, railways, waterways and pipelines, each of which is critical to ensuring the freedom of mobility and economic growth," said Secretary Ridge. "These projects are critical to the mission of securing our ports."** The Transportation Security Administration, the United States Coast Guard and the Department of Transportation's Maritime Administration evaluated the Port Security Grant Applications and selected the grant award recipients. The latest round of grants has been awarded to 442 projects in 326 locations to 235 applicant organizations from across the nation.
Source: http://www.dhs.gov/dhspublic/display?content=2568

8. *December 10, Associated Press* — **Train conductors stole thousands. Five former Amtrak conductors working out of the Rensselaer station were sentenced for stealing money from the company. The five have been ordered to repay the more than $120,000 they stole by pocketing cash from tickets sold aboard their trains.** The men were also sentenced Tuesday in Albany federal court to five years' probation after pleading guilty last summer to charges that they each stole more than $5,000 from Amtrak over the past several years. The thefts of cash from on−board ticket sales were uncovered during a routine audit. Prosecutors said Amtrak is conducting audits of ticket sales all over the country and others have been charged. The former conductors were from the Albany area, western Massachusetts and Virginia.
Source: http://www.capitalnews9.com/content/headlines/?ArID=51105&Se cID=33

9. *December 10, Capital News 9 (Albany, NY)* — **The search continues for crew members. Rescue crews are back to work at the Port of Albany today −− fighting the frigid Hudson River to search for three missing crew members of a Dutch cargo ship. A massive crane has been situated near the vessel −− Tuesday the crane was part of the operation and recovery.** Wednesday morning it was used to pickup a tug boat −− the Erin Miller. It is being used to probe the area around the ship. A Coast Guard vessel has been moving around the

waters to see how close it can get to the ship without disrupting the position of the vessel. **The Coast Guard Commander said that crews have been working hard to make sure that the water pollution from the diesel fuel is kept to a minimum. He said officials are optimistic that pollution will be limited due to the lower tide that is expected later today.** Officials also said that weight limits didn't appear to be exceeded, so another big part of this operation is trying to find out exactly what went wrong. The Port of Albany is closed for a one−mile radius around the ship −− no boats in or out. There are several boats sitting at the one−mile line waiting for instructions. The vessel, which had come from the Netherlands, was being loaded with 600 tons of turbine equipment bound for Italy and Romania when the cargo shifted and caused the barge to capsize.
Source: http://www.capitalnews9.com/content/top_stories/default.asp? ArID=51134

10. *December 10, National Journal's Technology Daily* — **Customs officials may use sensors to test containers.** The Department of Homeland Security plans to deploy new technology at the nation's borders to inspect certain containers entering the United States. The department's division on customs and border protection soon will test the technology at the nation's Northern and Southern borders, Aaron Diaz, a staff scientist with Pacific Northwest National Laboratory, said during a press briefing on new technologies for national defense. **The hand−held, drill−shaped device uses an advanced, ultrasonic sensor system to detect suspicious liquids or solids in containers, Diaz said. It sends sound pulses from wall to wall of containers and within three to five seconds can alert officials via a tethered digital assistant of possible contraband or terrorist threats.** While the device has been on the market for only one year, it incorporates 60−year−old technologies, Diaz said, adding that earlier versions were employed during treaty verifications to identify chemical and nuclear weapons. And he said U.N. weapons inspectors used the latest version in Iraq before the war.
Source: http://www.govexec.com/dailyfed/1203/121003td1.htm

11. *December 10, Government Executive Magazine* — **Air traffic controllers agree to two−year contract extension. The National Air Traffic Controllers Association (NATCA) and Federal Aviation Administration (FAA) have reached an agreement on a two−year contract extension for more than 15,000 workers, the organizations announced Monday.** The agreement binds more controllers than ever to a performance−based pay system and allows the FAA to adjust staffing levels at airports around the country based on workload. It also modifies certain pay rules for controllers and changes several memoranda of understanding the FAA and union previously negotiated. The FAA estimates the agreement could save the government as much as $40 million over the next four years. "The FAA is becoming a more performance−based organization, and this extension is a significant component of that effort," said FAA Administrator Marion Blakey. "This agreement helps us focus on the needs of the traveling public and the taxpayer." NATCA President John Carr called the agreement a "win−win situation for the flying public." Union spokesman Doug Church said NATCA considers its contract to be one of the best in government.
Source: http://www.govexec.com/dailyfed/1203/121003c1.htm

[Return to top]

Postal and Shipping Sector

12. *December 10, Today's Trucking* — **Shareholders approve LTL merger.** Yellow Corp.'s acquisition of Roadway Corp. moved forward Tuesday as shareholders of both trucking companies approved the cash−and−stock deal that had been valued at $966 million. **The transaction, which will likely close tomorrow, will result in creation of Yellow Roadway Corp., which would control more than 15 percent of the U.S. less−than−a−load (LTL) market as a result of the merger.** The combined $6 billion Yellow and Roadway took in last year would make the joint company North America's third−largest ground transportation company, behind UPS and FedEx Corp. The new company and Yellow will merge some administrative operations but will continue to operate as separate entities.
Source: http://www.todaystrucking.com/displayarticle.cfm?ID=2798

[Return to top]

Agriculture Sector

13. *December 10, Billings Gazette* — **U.S. proposes plan to vaccinate bison. The Animal and Plant Health and Inspection Service (APHIS) is seeking approval for a plan that would allow state and federal workers to inject bison calves and yearlings with a vaccine in an effort to reduce the spread of the brucellosis in the area. Brucellosis is a contagious bacterial disease that can affect bison, elk, and cattle.** In infected animals, the disease can cause abortions, infertility, and other problems. Federal officials estimate that 35 to 50 percent of bison in Yellowstone may be infected with the disease. That notion led to a federal and state plan in 2000 intended to limit contact between Yellowstone bison and cattle that graze just beyond the park's boundaries. The plan gives agents the authority to push bison back into Yellowstone when they wander out in search of food. The APHIS proposal would allow young bison that are captured outside the park to be vaccinated for brucellosis. "This would reduce the potential threat of infection with brucellosis for cattle," the proposal says. **While the APHIS plan specifically targets bison, it mentions that a vaccine program for elk "will likely be considered" when a comprehensive brucellosis eradication program is developed for the Yellowstone area.**
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2003/12/10/build/wyoming/30−brucellosis.inc

14. *December 10, Joong Ang Daily* — **Calves said to resist mad cow disease. A team of Korean veterinarians Tuesday presented what it believes to be the first calves that are resistant to mad cow disease. The calves were cloned with the removal of a protein known to cause the deadly neurological disease in cows.** The first of the four calves was born on November 15, with the last birth coming on November 29. There are currently 15 surrogate cows pregnant with more of the cloned calves. Hwang Woo−suk, a Seoul National University professor who led the research, said tests show the four calves have a gene that suppresses the growth of the prion protein, believed to be the agent that transmits the disease to cows. They were cloned from the eggs of a single natural mother after the gene that produces the prion protein had been replaced with a similar but harmless gene. **The calves will be sent to the National Institute of Animal Health in Tsukuba, Japan for a joint clinical study by Korea and Japan, since Korea lacks the facilities for the study.** With most cases of the disease developing in cows between the ages of three and five, the study will have to be conducted for at least three years so that reseachers can watch for an outbreak.

Source: http://joongangdaily.joins.com/200312/11/200312110150035579900090409041.html

[Return to top]

Food Sector

15. *December 09, Reuters* — **U.S. green onion hepatitis linked to Mexico. Federal health investigators have determined that a deadly outbreak of hepatitis A among restaurant diners in Tennessee, Georgia, and Pennsylvania was caused by green onions produced in Mexico, the U.S. Food and Drug Administration (FDA) said on Tuesday.** More than 500 people were infected in the outbreak and three died. FDA investigators pinpointed a link between the three outbreaks and green onions from Mexico after visiting four Mexican companies last week. They found poor sanitation and inadequate hand washing facilities and also had concerns about the quality of water used in the fields, packing sheds, and the making of ice, which can help spread the disease. A fourth outbreak of hepatitis A occurred at a North Carolina restaurant, but health department workers have not finished their traceback investigation. **The investigation has been difficult because no reliable methods exist to find the virus in green onion samples collected in the field. Instead, health workers analyzed the hepatitis A viruses in infected consumers and found they were virtually identical to those found in residents who live along the U.S.−Mexican border.**
Source: http://www.forbes.com/markets/newswire/2003/12/09/rtr1175013 .html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

16. *December 10, United Press International* — **Progress made in developing Ebola vaccine. Army scientists reported Tuesday developing Ebola virus−like particles that prevent lethal Ebola virus infections in mice.** The scientists say they've successfully immunized mice against the Ebola virus using hollow virus−like particles, or VLPs, which are non−infectious, but which are capable of provoking a robust immune response. The work could serve as a basis for development of vaccines and other countermeasures to Ebola, which causes hemorrhagic fever with fatality rates as high as 80 percent. **Ebola is of concern both as a global health threat and a potential agent of biological warfare or terrorism. Currently there are no available vaccines or therapies.**
Source: http://washingtontimes.com/upi−breaking/20031209−085803−2370 r.htm

17. *December 09, United Press International* — **CDC may buy flu vaccine from Europe.** Federal health officials said Tuesday the flu vaccine shortage in the U.S. has become so severe they are looking to obtain additional doses from Europe. **The U.S. Centers for Disease Control and Prevention (CDC) plans to "look at how we can first of all purchase whatever doses are**

remaining ... not only here in the United States, but licensed vaccine in Europe," Dr. Julie Gerberding, director of the CDC, said. The European vaccine is made by Chiron, which manufactures the medication in the U.S. and also has offices in Germany and Italy. "We're exploring whether that vaccine could be cleared for use in the United States" in time to be used during this flu season, Gerberding said. Last week, the CDC announced the two major U.S. vaccine manufacturers, Aventis Pasteur and Chiron Corp., had distributed all of the 83 million doses of vaccine they made for this year's flu season. **In addition, the CDC is working with state and local health officials to get an idea of how many doses of vaccine are still available. Some areas have vaccine shortages while it appears to be abundant in others, Gerberding noted.**
Source: http://www.upi.com/view.cfm?StoryID=20031209−021442−7955r

18. *December 09, Food and Drug Administration* — **Lab culture test for anthrax. The Food and Drug Administration (FDA) Tuesday cleared a test kit for clinical laboratories to use with culture testing to help distinguish the organism that causes anthrax disease, Bacillus anthracis, from similar organisms.** The Redline Alert test is intended to be performed with other laboratory tests and procedures on a laboratory culture of bacterial cells from people who may have been infected with B. anthracis. The test helps determine whether or not a person has anthrax disease. **"Today's approval of a lab test for anthrax infection is another first step forward in our urgent mission to protect Americans from biological weapons," said Mark B. McClellan, Commissioner of the FDA.** The Redline Alert is an additional tool that laboratories can use to more easily identify B. anthracis. The test is easy and simple to use. Once cells are growing in the lab cultures, it can be performed in about 15 minutes and does not require specially trained personnel or special instrumentation. Other identification tests now used by laboratories may require overnight testing or special equipment and specially trained personnel.
Source: http://www.fda.gov/bbs/topics/NEWS/2003/NEW00992.html

[Return to top]

Government Sector

19. *December 10, Associated Press* — **Kelleher, Romney, Cilluffo named to Homeland Security Advisory Council.** Southwest Airlines Chairman Herb Kelleher has been named to a panel that recommends security measures to the Homeland Security Department. Massachusetts Gov. Mitt Romney and Frank J. Cilluffo, who manages George Washington University's homeland security programs, were also appointed to the Homeland Security Advisory Council. **The council, with representatives from state and local governments, universities and corporations, provides recommendations to Homeland Security Secretary Tom Ridge, who announced the appointments Monday.** Kelleher founded and served as chief executive of Dallas−based Southwest until 2001. He was named vice chairman of the homeland security group's private sector advisory committee. Romney was chief executive of the organizing committee for the 2002 Winter Olympics in Salt Lake City before being elected governor of Massachusetts in 2002. Cilluffo served as special assistant to President George W. Bush for homeland security and spent eight years as a policy analyst with the Center for Strategic & International Studies in Washington.
Source: http://www.thebostonchannel.com/politics/2696282/detail.html

[Return to top]

Emergency Services Sector

20. *December 10, Huron Plainsman (South Dakota)* — **South Dakota has homeland security presentation.** It's a mistake to assume that a terrorist incident couldn't happen in such an isolated place as South Dakota, the coordinator of the state's Joint Terrorist Task Force said Saturday in Huron. "Why strike in South Dakota?" FBI special agent Dan Reynolds of Sioux Falls asked at the annual meeting of the South Dakota Association of Towns & Townships. "My attitude is, why not strike in South Dakota? What better way to send a message that no place is safe if you do a terrorist incident in America's heartland?" he said. Reynolds, a 19−year veteran of the FBI, and Dave Heller, a special agent for 14 years, did a presentation on homeland security. **The task force, established about a year ago, has representatives from the FBI, Minnehaha County Sheriff's office, Immigration and Naturalization Service, Transportation and Safety Administration and the Sioux Falls Police Department.** A large influx of immigrants, especially in Sioux Falls, is a source of concern, Reynolds said. **Refugees are from Somalia, Iraq, Libya, Sudan and Ethiopia, all countries that in the past have supported terrorist activities, he said. The task force worries about terrorist activity linked to international groups as well as domestic ones.**
Source: http://www.zwire.com/site/news.cfm?newsid=10642458&BRD=1128&PAG=461&dept_id=97933&rfi=6

[Return to top]

Information and Telecommunications Sector

21. *December 10, eWEEK* — **Security experts warn of new way to attack Windows.** Security experts have found a new way to exploit a critical vulnerability in Windows that evades a workaround. Microsoft Corp. issued a patch for the vulnerability in November, but the security bulletin also listed several workarounds for the flaw, including disabling the Workstation Service and using a firewall to block specific UDP and TCP ports. Researchers at security company Core Security Technologies discovered a new attack vector that uses a different UDP port. This attack still allows the malicious packets to reach the vulnerable Workstation Service. **An attacker who successfully exploits the weakness could run any code of choice on the vulnerable machine. An attacker doesn't have to individually address computers on the network, but can broadcast an attack. Such a tactic could actually create a worm that spreads faster than the SQL Slammer worm did last year.** Microsoft urged customers to apply the patch. "Applying the patch does correct the problem," said Iain Mulholland, a security program manager for Microsoft.
Source: http://www.eweek.com/article2/0,4149,1408902,00.asp

22. *December 10, Government Computer News* — **IPv6 will need security, too, experts warn.** Security has been one of the selling points for the new Internet protocol, but IPv6 is not inherently secure, say those planning its implementation. The Internet Engineering Task Force is still working on IPv6 security elements and “many of them need to be tested in the real

world," security consultant Richard Graveman said Wednesday, December 10, at the U.S. IPv6 Summit in Arlington, VA. **One of the key security elements in IPv6 is IPSec encryption, which is mandatory in the new protocol. But security is more than IPSec, Graveman said. "Downloading an encrypted virus and installing it is just as bad as downloading an unencrypted virus," he said. Good encryption will not stop hackers either, he said**. "You don't break good crypto, you go around it," he said, so proper implementation of IPv6 and a secure platform still are key to securing networks. Latief Ladid, president of the IPv6 Forum, said warned that **hackers already are studying the new protocols and are uncovering security flaws**.
Source: http://www.gcn.com/vol1_no1/daily-updates/24398-1.html

23. *December 10, Dow Jones Business News* — **SCO Group Website disabled by another hacker attack.** The Website of SCO Group Inc. has been temporarily disabled by a hacker attack that began early Wednesday, December 10, the company said. **It marks the third time this year the Lindon, UT, software firm's site has been the target of a "denial of service" attack**. In such assaults, hackers bombard an Internet site with traffic in an attempt to overwhelm its server computers and shut it down. The latest attack began at 6:20 a.m. EST, and it isn't clear when it will cease, said SCO spokesman Blake Stowell. Past attacks against the company's site have lasted for several days. Stowell said the company has notified law-enforcement authorities. **The attack is preventing SCO customers from downloading updates or security fixes to their software**.
Source: http://biz.yahoo.com/djus/031210/1527001248_1.html

24. *December 09, Government Computer News* — **Moonv6 testing to continue. Initial ten-day testing in October on the nation's largest native IPv6 network by the Department of Defense (DoD) and the University of New Hampshire demonstrated IPv6 linkage of academic and military sites from New Hampshire to San Diego. Time was short, and there was a dearth of applications written for the new Internet Protocol**. "We had a limited number of vendor implementations to work with," said Ben Schultz, managing engineer of the University of New Hampshire's interoperability laboratory. Opportunities to test security also were limited, he said Tuesday, December 9, at the U.S. IPv6 Summit in Arlington, VA. Under those constraints, the File Transfer Protocol, Hypertext Transfer Protocol, Secure HTTP, Telnet and Domain Name System applications worked, Schultz said. **The Moonv6 test bed is a collaboration by JITC, the university lab and the North American IPv6 Task Force.** The second phase of testing, scheduled to run from February 2 to April 14, will dig deeper into security, mobility and routing protocol testing, as well as network stability and management, JITC's Major Roswell Dixon said.
Source: http://www.gcn.com/vol1_no1/daily-updates/24375-1.html

25. *December 09, Government Executive* — **Agencies get failing grades on cybersecurity .** Federal efforts to secure critical computer systems and sensitive information are improving, but more than half of all agencies are still doing very poorly at the task, lawmakers said Tuesday, December 9. Overall, **the federal government received a grade of D for cybersecurity, up from a grade of F a year earlier, according to the 2003 Federal Computer Security Scorecard released Tuesday**. The scorecard, which is compiled by the House Government Reform subcommittee, is based on information reported by each agency and federal inspectors general to Congress and the Office of Management and Budget. Senator Susan Collins

(R−ME), who chairs the Senate Governmental Affairs Committee, urged agencies to take immediate action to improve cybersecurity. **"The administration has reason to believe that cyberattacks could be part of terrorists' game plans," she said. "We cannot afford to be caught off guard."**
Source: http://www.govexec.com/dailyfed/1203/120903c1.htm

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 1433 (ms−sql−s), 445 (microsoft−ds), 80 (www), 137 (netbios−ns), 554 (rtsp), 21 (ftp), 53 (domain), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

26. *December 10, Australian Associated Press* — **Malaysia detains Jemaah Islamiah suspects. Malaysia has issued two−year detention orders on five students who allegedly trained in Afghanistan and Pakistan as a new generation of leaders of the South−East Asian Jemaah Islamiah (JI) terrorist group. A Malaysian intelligence officer said the five detainees had been sent to an Islamic school in Pakistan by Hambali, the detained operations chief of the al Qaeda linked JI.** They were among 13 students arrested and deported by the Pakistani authorities on November 10. The other eight students have been released, though four have been placed under restriction orders limiting their movements. **The five jailed students had been trained to carry out bombing and suicide attacks against U.S. interests in Malaysia and worldwide, the official said.** While studying in Pakistan they had joined a secret JI−linked group, the al−Ghuraba, and were believed to have attended sermons by international terrorist Osama bin Laden. Malaysia is holding around 80 terror suspects. Many are allegedly members of JI, which is accused of responsibility for a series of attacks including the Bali bombing last year which killed 202 people.
Source: http://www.theage.com.au/articles/2003/12/10/1070732287196.h tml

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer